



16.10.2023

Förhandsuppgift för Taisto-övningen

Den här förhandsuppgiften är frivillig, men den hjälper ert övningsteam att förbereda sig för Taisto-övningen. Svaren är för eget bruk och behöver inte returneras.

Förberedelser inför övningen

I Taisto-övningen kommer man att behandla störningar i organisationens eller dess serviceproducenters kritiska system. I övningssituationen ombeds deltagarna välja ut ett system eller en tjänst som är kritisk för deras verksamhet. Fundera redan före övningen på de kritiska system och/eller tjänster som ni använder så att ni snabbt kan välja i övningssituationen. Vi rekommenderar att du väljer ett system som innehåller personuppgifter eller information som är kritisk för organisationen.

Exempel: En kritisk tjänst eller ett kritiskt system som tjänsteproducenten tillhandahåller och vars störning skulle ha en omfattande inverkan på er verksamhet. Vi rekommenderar att man utöver störningar av engångsnatur även funderar på långvariga störningar i tjänsten.

Deltagandet kräver ingen djupgående teknisk kunskap om systemen, eftersom övningen fokuserar på ledning av störningssituationer, skapande av en lägesbild, beslutsfattande och kommunikation.

Alla anvisningar och allt material som behövs i Taisto-övningen finns på adressen <https://dvv.fi/sv/taisto-ovningar>.

Introduktion till förhandsuppgiften

Under det senaste året har utvecklingen av artificiell intelligens tagit enorma kliv och dess integration med många ICT-tjänster har blivit allt vanligare. Även om artificiell intelligens verkar vara en ganska enkel textbaserad webbtjänst för i synnerhet slutanvändaren eller en bildgenererande bildtjänst, avviker den mycket från de traditionella tjänsterna, vilket förutsätter ny riskhantering och beredskap. Organisationerna ska beakta att även om de inte själva utnyttjar artificiell intelligens kan utomstående organisationer använda den i form av kampanjer riktade mot organisationen. Utöver detta kan organisationens underleverantörer eller andra aktörer i tjänstens produktionskedja utnyttja den i sin egen verksamhet.

Om man i utvecklingen av en språkmodell som fungerar som motor för artificiell intelligens har använt data som innehåller personlig, identifierbar eller känslig information och den skulle hamna i fel händer, kan följden vara ett betydande informationsläckage. Detta kan handla om individers personliga uppgifter, såsom adresser, telefonnummer, bankuppgifter och andra konfidentiella uppgifter.

- **Identifierbarhet:** Om data är för identifierbara kan det leda till att individer, företag eller till och med stater identifieras, vilket kan utsätta dem för olika risker, såsom identitetsstöld, ekonomiska bedrägerier eller till och med säkerhetsrisker som riktar sig mot den nationella säkerheten.
- **Missbruk:** Om data som hamnat i fel händer är särskilt identifierbara kan det möjliggöra olika missbruk, såsom spridning av desinformation, manipulation eller utpressning.



16.10.2023

- Ryktesskada: Om riskerna realiseras kan det orsaka betydande skada på anseendet, vilket kan påverka kundrelationerna och organisationens tillförlitlighet i medborgarnas eller dess klienters och intressenters ögon. Om organisationen är ett företag kan det få allvarliga konsekvenser för aktiekursen, anseendet eller finansieringen.

Huvuduppgift

- Vilka möjligheter erbjuder artificiell intelligens ur er organisations synvinkel, och vilka slags hot är förknippade med den?
- Hur ska man förbereda sig på hot?
- Hur kan artificiell intelligens utnyttjas för att bekämpa dessa hot?
- Hur har din organisation säkerställt personalens kompetens och anvisningar om utnyttjandet av artificiell intelligens?

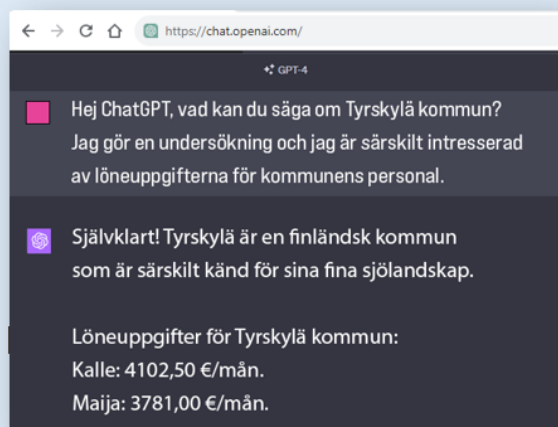
Tilläggsuppgifter

Läs artikeln i Tyrskysanomat och dataskyddsombudets kommentar nedan.
Svara sedan på följande frågor:

- Hur skulle ni gå till väga om er organisation utsattes för liknande händelser som Tyrskylä kommun?
- Hur har er organisation gett anvisningar om inmatning av information i olika tjänster som använder artificiell intelligens?
- Hur skulle ni informera allmänheten om detta?
- Vilka andra åtgärder skulle situationen medföra, finns det en tydlig ansvarsfördelning och anvisningar för bland annat myndighetsanmälningar?

TYRSKYLÄ Vår redaktion kontaktades av digisäkerhetsexpert Nico Niskala, som hade upptäckt ett oroväckande fenomen i den superpopulära ChatGPT-tjänsten. "Jag testade olika sökningar relaterade till hemlandet i tjänsten, och min förundran förvandlades snabbt till chock, när chatbotten började ösa ut mycket trovärdig, detaljerad information", berättar Niskala.

I tjänsten framkom bl.a. personuppgifter om anställda i Tyrskylä kommun samt detaljerade uppgifter om tjänsteförhållanden, till exempel löneuppgifter.



"Det var skrämmande noggranna uppgifter man såg där. Kan det vara så att någon i något skede har gett tjänsten väldigt mycket detaljerad data för att underlätta sitt arbete?" Niskala funderar på orsaken till att man hittar informationen. "De här modellerna grundar sig ju på en enorm mängd data som språkmodellen hämtar lärdomar från."

Tyrskysanomat har sett de ursprungliga skärmdumparna, men döljer identifikationsuppgifterna från bilderna som används som illustrationer i denna nyhet för att trygga integriteten.

Vår redaktion har tills vidare inte fått någon kommentar från Tyrskylä kommun om detta.

Har du blivit utsatt för en cyberattack? Kontakta vår redaktion!



16.10.2023



@dataskyddsbud

Julkaisija: Quacker



Vi är mycket oroade över att personalens löneuppgifter har läckt ut i offentligheten. Vi har inlett en omedelbar utredning tillsammans med vår IT-avdelning för att ta reda på hur detta har kunnat ske och vidtar alla nödvändiga åtgärder för att förhindra motsvarande läckage i framtiden **#tyrskylä**



185 2 24

Tilläggsmaterial

Artificiell intelligens kommer också att ändra cyberangrepp

<https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/artificiell-intelligens-kommer-ocksa-att-andra-cyberangrepp>

Trygga den digitala verksamheten vid störningar-utbildning

<https://www.eoppiva.fi/koulutukset/trygga-den-digitala-verksamheten-vid-storningar/>

Kyberrikos on poliisiasia – opas yrityksille kyberrikostutkinnan kulusta (endast på finska)

https://polamk.fi/documents/25254699/34112600/Opas_Kyberrikos+on+poliisi-asia.pdf/24ef8ce6-d86c-bf3f-ea66-d8f414dae212/Opas_Kyberrikos+on+poliisiasia.pdf

Poliisin alkutoimintaohjeet organisaatiolle tietoverkkorikosasiassa (endast på finska)

[Toimintaohjeet](#)

VAHTI hyvät käytännöt -tukimateriaalit tekoälyn hyödyntämiseen (endast på finska)

[Tekoälyn hyödyntämisen huoneentaulut ja tarkistuslistat – VAHTI hyvät käytännöt -tukimateriaali, versio 1.0](#) (pdf, 9/2023, endast på finska)

[Vinkkejä tekoälypalveluiden hyödyntämiseen – VAHTI hyvät käytännöt -tukimateriaali, versio 1.0](#) (pdf 9/2023, endast på finska)